National College of Ireland

Threat Handling using the NIST Framework in a Recruitment Environment

MSc Research Project
Cyber Security

Harshal Meher
Student ID: X19193521

School of Computing
National College of Ireland

Supervisor: Prof. Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Harshal Rajendra Meher

Student ID: X19193521

Programme: MSc in Cybersecurity **Year:** 2020-2021

Module: Industry Internship

Supervisor: Prof. Vikas Sahni

Submission Due Date: 06/09/2021

Project Title: Threat Handling using the NIST Framework in a Recruitment Environment

Word Count: ……6299…… **Page Count**……21……..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Harshal Rajendra Meher

Date: 05/09/2021……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Threat Handling using the NIST Framework in a Recruitment Environment

Harshal Rajendra Meher
X19193521

Abstract

With a rising number of threats in the industry, small and mid-sized businesses experience several difficulties in managing the security of the information management systems. It has become essential to have a robust security service, such as a Security Operation Centre (SOC), that can monitor and detect threats. It is difficult for most small and mid-sized organizations to setup such dedicated security services because of the less IT budget. In recent years, the National Institute of Standards and Technology (NIST) has continued to create security management standards to help agencies in securely building integrated and company systems to manage data security. In this research, an integrated system that can identify malicious or suspicious activities inside a data management system and offer information security in a recruiting environment has been developed. This paper provides a brief description of the integrated system developed by following the NIST detection function and presents a hybrid model to detect suspicious events in the data management system. The final portions of this paper describe the experiments carried out while establishing this system in operation. The designed system is efficient in monitoring data storage systems and generating alerts when malicious or suspicious activity is detected.

Keywords: Security Operation Centre, NIST, Threat, Information Security

1 Introduction

Information Technology (IT) security is a combination of cybersecurity methods that protect against unauthorized access to corporate resources such as systems, networks, and information. It protects the integrity and confidentiality of sensitive data by preventing sophisticated hackers from accessing it. As hackers become more sophisticated, the necessity to safeguard your digital assets and network equipment becomes more critical. While implementing IT security might be costly, the expense of a large breach is considerably greater. IT teams can use an incident response plan as a risk management strategy for controlling the situation, during or after an event. Some large organizations may already have the necessary security measures implemented to prevent various cybersecurity threats but for the middle level or small organization, it is necessary to implement necessary security measures to prevent the data breach. Especially for the recruitment organization which processes sensitive data of the users, it is necessary to have a Security Operation Center (SOC) environment that can Detect, Monitor, and Report the threats in its IT environment.

The implemented solution focuses on the confidentiality, integrity, and availability of the data processed in the recruitment systems. This research aims to provide an integrated

architecture to Detect, Monitor, and Report Threats by following the detection function from the NIST guideline.[1] The detection function highlights the anomalies, events, security continuous monitoring, and detection process in NIST guidelines. Before implementing a SOC environment it is necessary to consider existing technologies, networks, and the data which is processed. Due to the variety of applications used in the infrastructure its necessary to implement monitoring and alerting systems. To achieve this an integrated architecture is implemented which comprises multiple technologies like Microsoft Cloud App Security (MCAS), Salesforce, Cisco Meraki to monitor, detect and report malicious activity.

Table 1: NIST Functions [1]

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

2 Related Work

This section of the paper highlights the literature review of the research done in the security of IT infrastructure and describes the methods implemented by the authors.

2.1 Literature Review

This paper is published by authors (Schilling, A. and Werners, B., 2016). The authors of this paper proposed a multimodal optimization approach for successfully selecting security measures to protect IT systems and services. In this research, the authors followed an IT baseline protection catalogue of the German Federal Office which consists of about 500 threats and 1200 safety measures. The model proposed by the authors helps in selecting the security methods to prevent threats. The model proposed in this research follows the existing database from the IT baseline protection catalogues and provides a security solution from its database. The designed system does not have a feature to add new threats and security methods and authors state to implement these features in their future work. Also, this model does not provide real-time suggestions if there is any security breach observed.

[1] https://www.nist.gov/cyberframework/online-learning/components-framework

In this paper the authors (Weissman, D. and Jayasumana, A., 2020) had presented a framework to monitor the security-related events in the network infrastructure with IoT devices. The paper describes the classification of different attacks in the IoT network. The attacks considered while designing the proposed framework are Data Leakage, Unauthorized Access, Denial of Service, and Spoofed Information/Action. This paper also highlights the challenges faced by the authors while integrating IoT with different SOC types like Outsourced SOC, Hybrid SOC, and Integrated SOC. The integration of IoT devices with SOC is described in three frameworks, IoT security monitoring outsourcing, the development of different analyst teams within an organization, and full integration of IoT. The limitation of this paper is that here the authors have presented a framework that focuses only on IoT devices.

In this paper the author's (Xu Li and Liu Hongyan., 2010) investigated a telecommunication company and propose security majors for the company systems. This paper's authors illustrate the issues in information system security and propose solutions to these issues. The authors propose an infrastructure with IT service management systems. This paper didn't focus on the threats, mitigations, and the security majors as per the SOC environment. It describes the security policies required for a specific organization which is investigated in the research.

In this paper the authors (Huang, Y. et al., 2019) had developed a risk management system by following the NIST security controls. The authors aimed to develop a risk management system that can monitor, identify, and mitigate risks. This system enhanced the risk management process and automated the security controls evaluation process. The developed system in this research focused only on the risk management process and did not provide solutions for information security. The tool only helped to manage risk processes and did not detect the threats or vulnerabilities in real-time.

The authors (Akinrolabu, O., Agrafiotis, I. and Erola, A., 2018) of this paper conducted a literature review on malware analysis technologies, focused on the features included in these techniques, and expanded the feature set with unique ones found by interviews with professional SOC analysts. The results in this research indicated the presence of newer type malware features based on networks and application events, and researchers identified significant teachings for implementing a new SOC for their structure and procedures. They also examined and analyzed the qualitative data gained from interviews. The interviews conducted in this research aimed to collect information about the malware and techniques that followed to detect threats in a SOC. This research focused on multiple areas of SOC environment like analysis of network and application events, identifying malware behavior in different protocols, interviewing multiple SOC analysts to collect data of SOC operations and threats. The limitation of this research was it did not propose a solution to identify threats. However, this has been proposed by the authors in their future work.

In this paper the authors (Bin Hamid Ali, F. A., Jali, M. Z. and bin Nordin, M. N., 2021) discuss the types of threats and digital security in IT services. The primary focus of this research was to study digital security in Malaysia. The author highlights the incident statistics which includes the IT security threats like DOS, Intrusion, Spam, Vulnerabilities, etc. of three consecutive years 2017, 2018, and 2019. The security techniques proposed in this paper like Identification and Access, Encryption, Network Security, Firewall, etc are standard and straightforward. The author does not present any method of using these techniques and did not consider any attack vectors while mentioning these techniques.

In this paper the authors (Wenjun Cheng, Xiaosu Zhan and Shaohua Zhang., 2011) designed the service-oriented security architecture and security service core architecture for large-scale information systems. The service-oriented architecture (SOA) is a software architecture that uses the solution to match requirements. This architecture comprises multiple layers like security service core, basic security service layer, extended security service layer, and security application layer. The security service core architecture connects the service provider and users. The proposed design is only suitable for large-scale information systems.

In this paper authors (Tafazzoli, T. and Gharaee Garakani, H., 2016) had designed a framework for developing and administrating incident response in the company. Authors achieve this by analyzing events and system logs from the OpenStack. This paper only focuses on detecting threats in the cloud environment. The authors had designed a Cloud SOC architecture that consists of a threat detection system called Sitra. In the proposed architecture the authors have used Zabbix as a sensor and to transfer events to Sitra. This proposed system only focuses on cloud-related threats and did not provide a proper evaluation of the test performed on the system. This paper lacks the artifacts of the tests performed on the Openstack environment.

The authors (Gupta, N., Traore, I. and de Quinan, P. M. F., 2019) in this paper had developed a system to automate the threat analysis of IDS and SIEM systems. The authors developed an event classification system that identifies characteristics using graphical analysis and events using a deep neural network model. This paper only focuses on the exaction of important events from the SOC systems and provides the accuracy for only SOC event classification. This study focuses solely on the extraction of significant events from SOC systems and delivers accuracy just for SOC event categorization.

Authors (Duan, J., Zhao, B. and Guo, S., 2020) had implemented a Smart Grid SOC framework that analyzes the data in real-time and provides interactive and batches analysis. The authors have segmented the implementation on building the SOC platform, the architectural design scheme, and the implementation strategy. The designed smart grid SOC system is mainly developed to analyze operations and data on the cloud platform.

The authors (Ilya Livshitz, Pavel Lontsikh and Sergey Eliseev, 2017) in this paper had proposed a method to assist the IT security in the organization. The methodology described by the authors follows guidelines from international ISO standards. The methods developed

by the authors are limited to financial organizations and focuses on risk assessment standards. The information and security measures used to secure the data stored in a given application are not proven in this study.

Authors in this paper (Minkevics, V. and Slihte, J., 2017) had addressed the problems related to security in an academic environment. They propose a risk management system to improve the security in the infrastructure and prevent security-related issues. The researchers also present the decision-making process to simplify the system and automate the threat detection module. The system developed in this research only provides the mitigations to social engineering attacks. Also, the system lacks in generating logs and the analysis of the risk is done manually by the security officer which is time-consuming. The proposed system is expensive, but the authors have outlined a future scope to make it more cost-effective.

A concept for the development of an IT security measuring technique was developed and reported in this research (Heidenreich, M., 2020). The researcher designed an application-oriented methodology intending to address micro-companies, particularly craftwork organizations. The basic specification for the design and features of the semi-automatic measuring approach with manual data collecting was described. This research falls short of giving a comprehensive investigation of the results. However, the same has been proposed by authors in their future work.

This paper (Soni, K. and Vala, B., 2017) describes security levels present in the Salesforce platform. The authors have highlighted the use of security features like internal data security, SSO, permissions, organizational settings, multi-factor authentication, profiles, and field-level security. This research concentrates solely on the security feature offered by the Salesforce application and emphasizes the elements to avoid a security breach. The authors also present the Salesforce security model which consists of users, auditing, record-level security, authentication, encryption, and so on. Despite this level of security, the system lacks monitor the files that are stored in it, and there is no enterprise-level security system that can analyze and alert if there is a data breach.

2.2 Research Niche

This section of the report summarises the previous work and explains the significance of the implemented system in this paper. The previous research or development was primarily done by implementing a security system without adhering to any security standards or designing an architecture without addressing risks or security breaches in the infrastructure. In addition, several papers limited security to IoT devices while ignoring application-level security. These papers lack in emphasizing the process or methods used to detect threats in a database management system. In this research, the implemented system is capable of detecting, monitoring, and reporting vulnerabilities or threats in the database management application. The design system can also integrate numerous applications to monitor and investigate data.

Table 2: Previous research summary

References	Techniques	Methodology	Parameters focused
1	Designed Security architecture	IoT security monitoring outsourcing, the development of different analyst teams within an organization, and full integration of IoT	Limited to IoT devices
2	Designed Security architecture	Investigating current security functions followed in telecommunication company	Security in IT service management systems
3	Designed Security architecture	Designed service-oriented security architecture	Multiple layers in the architecture are security service core, basic security service layer, extended security service layer, and security application layer
4	Designed Security architecture	Designed threat detection system called Sitra	Analyzed events and system logs from the OpenStack
5	Designed Security system	Developed a system to automate the threat analysis in IDS and SIEM systems.	Analyze event logs from the SOC system
6	Designed Security system	Analysed the performance of the ElasticSearch	Analyse data on the cloud platform
7	Designed Security system	Use of IDS and Splunk for developing the risk management system	Analyse parameters related to the user, IP address, connection time, API calls.
8	Designed Security system	Used semi-automatic measuring approach to analyse data	Designed for very small organizations with 1-9 people
9	Following Standard Security Guideline	Followed an IT baseline protection catalog of the German Federal Office	Followed 500 threats and 1200 safety measures described in the guide
10	Following Standard Security Guideline	Developed a risk management system by following NIST security controls	Manage risk processes
11	Following Standard Security Guideline	Reviewing malware analysis technologies, describing the features by interviewing professional SOC analysts.	Focused on analysis of network and application events, identifying malware behavior in different protocols, interviewing multiple SOC analysts to collect data of SOC operations and threats
12	Following Standard Security Guideline	Analyse IT security threats like DOS, Intrusion, Spam, Vulnerabilities, etc. of three consecutive years 2017, 2018, and 2019	The security techniques proposed in this paper like Identification and Access, Encryption, Network Security, Firewall, etc are standard
13	Following Standard Security Guideline	Followed ISO standards	Limited to financial organizations and focuses on risk assessment standards

14	Following Standard Security Guideline	Described Salesforce security model	Focused standard Salesforce security parameters like auditing, record-level security, authentication, encryption

3 Research Methodology

This section of the paper explains the procedures that are followed while designing the SOC system. The implemented system in this project follows the NIST detection function to Detect, Monitor, and Report Threats. Using this function, anomalous activities are identified in a timely manner, and the potential impact of occurrences is evaluated. There are generally three directions that can be taken to implement a SOC environment an Internal SOC, Outsources SOC (Managed Security Service Provider), or Hybrid SOC.[2] As this is the starting phase of the implementation, an internal SOC environment has been implemented. The implementation follows three primary phases while developing a SOC system in a recruitment environment. The first step focuses on the analysis of the existing technologies in the industry that are used while implementing a SOC system. The second phase follows the deploying of integrated architecture and the third is the testing and evaluation phase.

3.1 Analysis of existing technologies:

It is crucial to understand the existing technologies, infrastructure, and data that will be analyzed in the system. The existing technologies like database management systems, network structure, operating patterns, and IT policies of the organization were studied. The recruitment organization uses Microsoft O365 for enterprise work and Salesforce application for storing user data on the cloud. The Microsoft O365 offers a Microsoft Cloud App Security service for security-related operations. [3] The Salesforce application stores user's data such as applicant resume, PPSN numbers (Personal Public Service Number), contact, and bank information. This information is frequently shared with authorized consumers. As a result, it is important to monitor the activities on the Salesforce platform. Considering the business requirement, the criticality of the data and to increase the security level of the Salesforce application an integrated architecture is developed to detect, monitor, and report threats in the recruitment environment.

3.2 Deploying Integrated Architecture:

This phase of the development describes the procedures followed while designing the architecture. Microsoft Cyber offers the information and guideline to enhance security in the organization. It highlights the information by following the security functions from the NIST framework.[4] Considering the business necessity to safeguard and monitor the activities on the Salesforce platform NIST detection phase was followed using the Microsoft Cyber offering. The detection function from the NIST framework focuses on the detection of anomalies and

[2] https://searchsecurity.techtarget.com/definition/Security-Operations-Center-SOC

[3] https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

[4] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWsccu

understanding the impact of the event. It also highlights the steps for continuous monitoring and identifies the cybersecurity events to establish security measures.[5] Using Microsoft for analyzing Salesforce events enables the multi-vendor environment by enhancing security and minimizing threats caused by bugs in a single vendor.

The implemented framework is an integration of Microsoft Cloud App Security and Salesforce to detect, monitor, and alert the activities performed on the Salesforce platform. MCAS offers various deployment modes including log collection, API connectors, and reverse proxy. It offers comprehensive transparency, controls over data transmission, and advanced analytics to detect and mitigate cybersecurity threats between all Microsoft and third-party cloud services (Salesforce).[6] The below flowchart shows the workflow of the implemented system. The event and activity logs from the Salesforce application are connected to MCAS using REST API. The activity performed on the data stored on the Salesforce is retrieved by the Microsoft App Connector. Further, these activity logs are analyzed and are compared with the policies configured on MCAS. The security policies are customized to detect threats and suspicious activities on Salesforce. These policies are categorized into Threat Detection, Information Protection, Conditional Access, and Shadow IT. These policies scan for multiple parameters like user information, source, and destination IP address, timestamp, data rate, file type, risky IP, malicious content, sensitive information, etc. from the event logs of Salesforce. If a certain event or activity matches the parameters configured in the policy an alert is triggered. These alerts are then investigated concerning the incident which generated the alerts. The investigation of these alerts can be carried out by considering six parameters which are security rating of the application, insights of file and user ID, Account details, OAuth applications, and activity logs. The investigative approach provides us with a thorough understanding of the alert while also helping us in taking the appropriate measures. In this was the MCAS is used to detect, monitor, and report threats or suspicious events on the Salesforce environment.

[5] https://www.nist.gov/cyberframework/detect

[6] https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

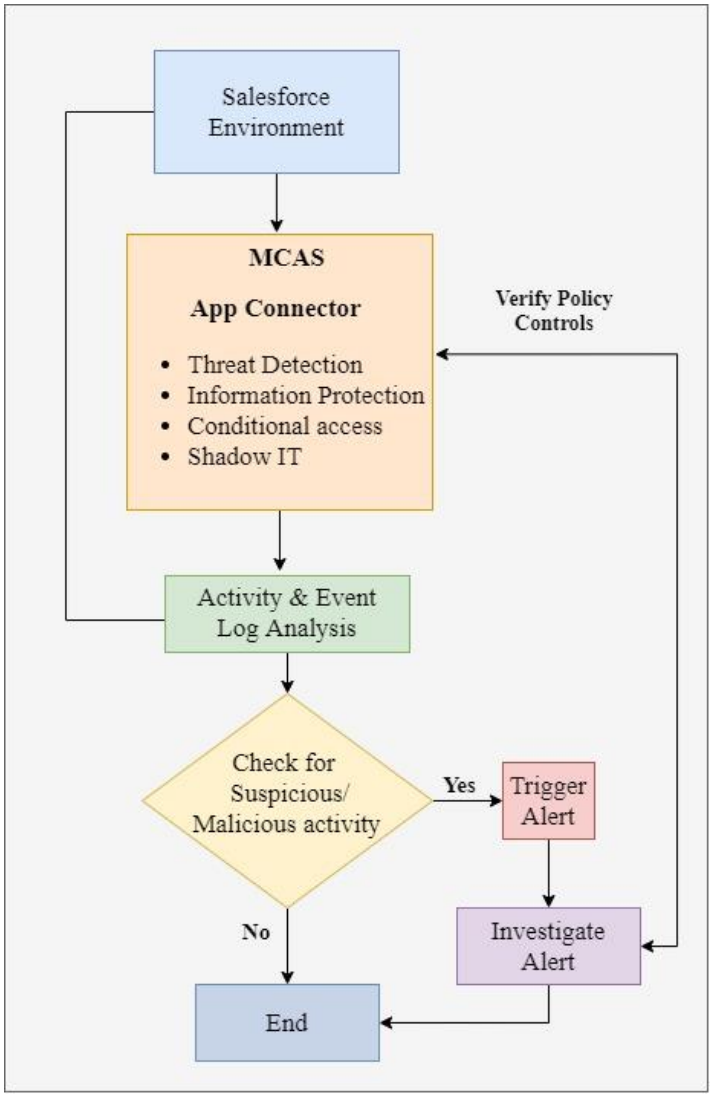

Figure 1: Workflow of integrated architecture

3.3 Evaluation:

In the phase of the project, the working of the system is tested. This phase highlights the behavior of each policy and the actions performed in response to the alerts. The complete description of this phase is covered in the **Evaluation** section of the paper.

4 Design Specification

The integrated architecture is developed to detect, monitor, and report threats in the required environment. This architecture follows the NIST Detection function to analyze events and to implement continuous monitoring. The section describes the tools and modules included in the architecture. The architecture integrates two cloud platforms Salesforce and Microsoft Cloud App Security. The activity and event logs on the Salesforce are retrieved in the MCAS with help of App Connector. This app connector can be used to connect multiple applications like Salesforce. It is composed of three major modules: Policy Control, Investigation, and Snapshot report/Continuous report.

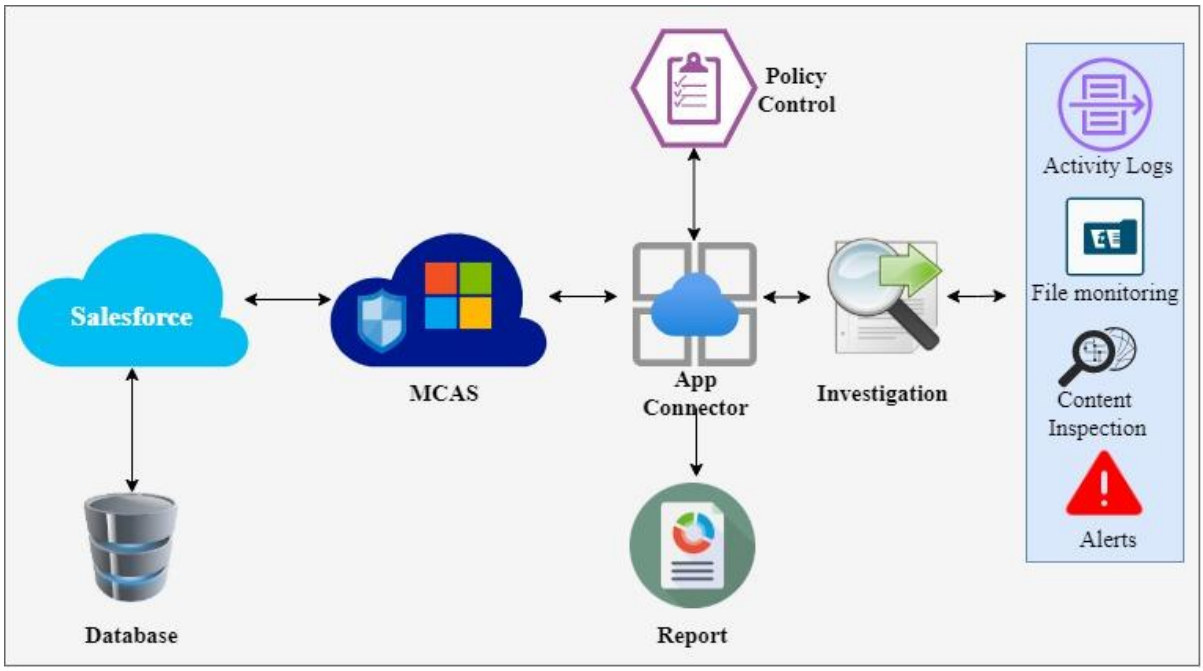

Figure 2: Architecture of the Integrated System

4.1 Policy Control Module:

The policies identify risky activity, breaches, and suspicious events or activities in the Salesforce environment. There are several categories of policies that can be configured to collect information from the Salesforce platform and these policies are used to remediate the actions. The types of policies that are configured are Activity policy, Anomaly detection policy, File policy, OAuth app policy, and Malware detection policy. These policies are categorized into Threat detection, Information protection, Conditional access, and Shadow IT. The configured policies can be further used for investigation.

4.2 Investigation:

The Investigation phase describes the investigation done on alerts and the data. This area highlights the key parameters of the data stored on Salesforce. It presents the details of the activity logs, Files, Data stored in the file, Section Apps, and the alerts generated with respect to the app connected.

4.2.1 Activity logs:

The events and activity logs are retrieved from the Salesforce application to the activity log section of the MCAS. Multiple policies are creates based upon the events and alerts are triggered if a policy match is found. These events help to understand the activities performed on a specific file and help us to identify suspicious activities. The activity logs also highlight the user ID, operation system or browser used, date, and location from where the activity is performed. The below image shows the details of malicious activity for the failed login attempt. It shows details like the User on who's the activity is performed, application of use, source IP address, device details, and so on. This activity can be used to investigate the details related to the user and the source IP address.

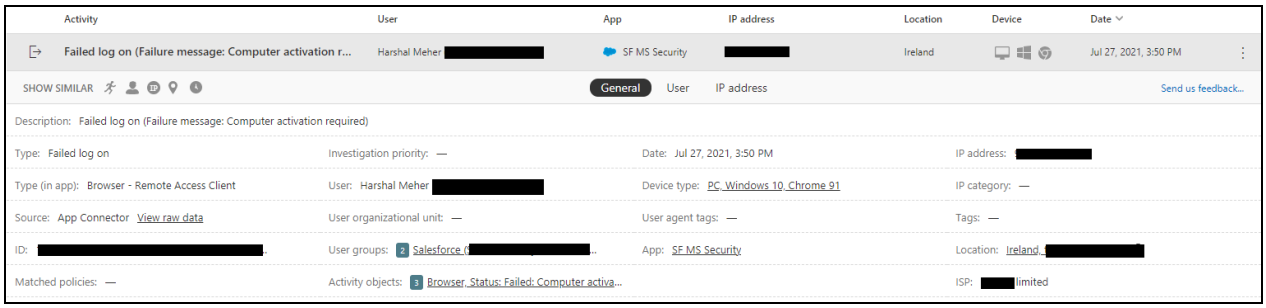

Figure 3: Activity log

4.2.2 File Monitoring:

When the Salesforce application is connected to the MCAS it scans for all the files on the Salesforce platform and rescans the files whenever it is altered. MCAS monitors files based upon metadata like file type and access levels. DLP module performs the content section and helps to identify crucial data inside the document. This module analyzes the malicious files containing hidden malware with the help of a malware detection policy. The below figure presents the details retrieved from a file.

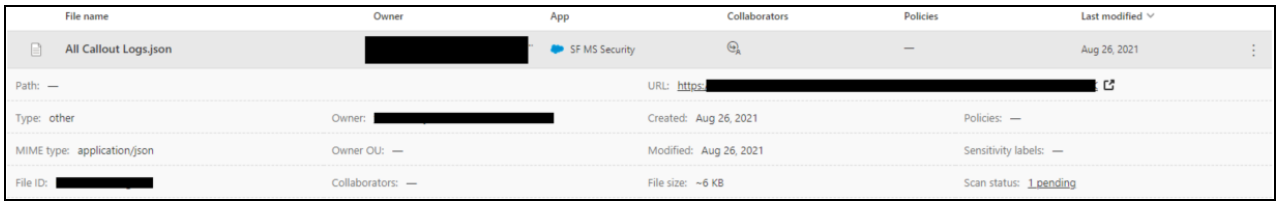

Figure 4: File details

4.2.3 Content Inspection:

The Content Inspection help to identify data leakage using DLP and Data Classification services. The data classification service helps to analyze the data inside the document using predefined Fingerprints and custom data matches. Using the DLP service the multiple permission can be configured to prevent files or data from unauthorized users. This service support decryption and encryption of files as and when required.

4.2.4 Alerts:

The alerts provide you a complete insight into any suspicious activity or policy violations. It helps to improve the security of the recruitment environment. A detailed description of the alert is mentioned in the **Evaluation** section of the report.

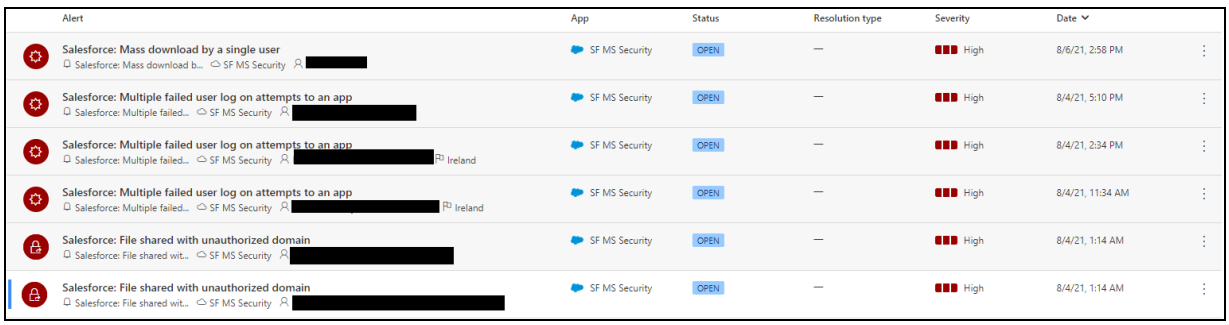

Figure 5: Alerts Generated

4.3 Reporting:

The reporting module in the MCAS helps to generate a snapshot and continues the report. This report provides an overview of the traffic logs on the Salesforce application. It highlights the suspicious and malicious activities and presents them in a simplified graph.

5 Implementation

This section of the report explains the implementation of the integrated system to secure the data stored in the recruitment industry. The Implementation of this system is first performed on the Sandbox environment of Salesforce and MCAS. The sandbox platform consisted of limited information and users configured. After successful integration and testing, the same steps were followed to implement the system in the live environment of the recruitment company.

This phase of the research primarily focuses on connecting the Salesforce environment with MCAS. The development of the integrated system followed two primary steps first to Connecting the Salesforce application to MCAS and second to Configuration of policies on the MCAS to analyse the data stored on Salesforce and identify the suspicious or malicious activities on the Salesforce platform.

5.1 Connecting Salesforce Application

The Salesforce application is connected to MCAS using the connector REST API. The App Connector on Microsoft used this API to retrieve the user activity data and events from the Salesforce platform. The REST API is enabled on the Salesforce application and necessary permissions are configured on the Salesforce to share the data with the MCAS platform. To add Salesforce on the Cloud App Security dashboard a dedicated profile with necessary privileges was created on Salesforce. This profile provided the necessary rights like to View all Data, Manage Salesforce CRM, Manage Users, Query All Files, and manage CRM data on the Salesforce platform. The Salesforce application was added to the App connector on the MCAS.

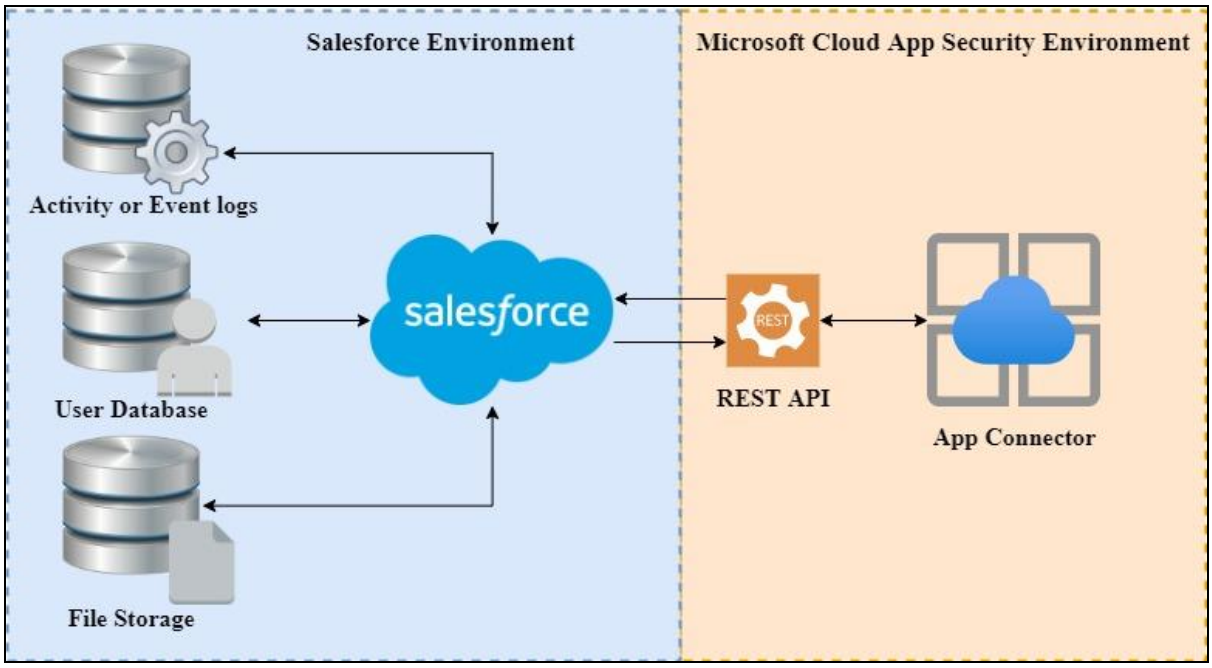

Figure 6: Connecting Salesforce to MCAS

5.2 Policy Configuration

The activities and events on the Salesforce platform are monitored on MCAS with the help of various policies. These policies help in identifying malicious and suspicious activities. When the thresholds and conditions set in these policies match the activity logs, an alert is triggered. These policies are categorized into four types Threat detection, Information protection, Conditional access, and Shadow IT policy. The policy can be configured in relation to user access, user session, activity, files, OAuth Apps, and anomaly detection. The configured policy can be disabled as required. The thresholds in the policy can also be used for single and repetitive activities. The severity of the policy is set to High, Medium, and Low depending upon the rate of impact. The filters inside the policy are used to filter the application, user, activity, file, and location. These policies are configured in such a way that they can send an Email to the IT team whenever an alert is triggered.
Some principal policies which are configured to detect malicious and suspicious activities are mention below,

- Logon from a risky IP address: Alert when a user logs on to the Salesforce application for a risky IP address. The database of the risky IP address is managed and maintained by Microsoft.
- Potential ransomware activity: This policy monitors the environment and sends alerts whenever an event pattern resembling a ransomware attempt is identified.
- File shared with unauthorized domain contains PPSN number: An alert is triggered if a file containing PPSN number is shared with the unauthorized domain. A list of internal and authorized users is configured in the MCAS.
- Multiple failed log-on attempts: This policy generates an alert if an attacker tries to brute-force the Salesforce login.
- Unauthorized user altering objects: The object configured on the Salesforce platform plays a crucial role in managing data fields. These objects are used to store and manage information on Salesforce. This policy triggers an alert when an unauthorized user tries to edit objects.
- Mass file downloads: When a single user downloads more than 20 files in one minute, an alert is generated.
- Mass file deletion: When there is a massive deletion of content delivery and content document links, this policy is activated.
- Sharing settings modified on Salesforce: To monitor the administrative activity on the Salesforce platform this policy is configured. This policy monitors the activities performed on sharing settings in Salesforce and an alert is generated if the settings are modified. To avoid the alerts of authorized users like system admin. The system admin account is filtered to avoid unnecessary alerts.
- Organizational activities from a non-corporate IP: The configuration changes are monitored, and the locations or IP addresses authorized to do the changes are whitelisted on MCAS. If an administrative activity is observed from non-corporate IP an alert is generated.
- Malware detection: Salesforce files are analyzed using Microsoft's threat intelligence engine, and if a file is detected as being associated with malware, an alert is generated.
- Impossible travel: This policy analyzes the application and sends alerts when the same user actions are identified in various places within a time period less than the estimated travel time between the two locations. This might imply that a distinct user is attempting to use the same credentials. Detecting this abnormal conduct needs a week's learning time during which it understands a new user's activities.

Cloud App Security supports in exporting the policies overview report which shows consolidated alert information per policy to use in monitoring, understanding, and customizing rules to safeguard the company.

6 Evaluation

This part of the research paper explains the testing done and the results obtained after implementing the integrated system. The system is tested in two stages. First, a sandbox environment is connected with MCAS, which contains limited data and users. Second, after configuring the system to the live environment. The sandbox environment was selected to minimize the impact of integration to the live environment.

6.1 Experiment on Sandbox Environment

In this first phase of the testing, the Salesforce sandbox environment is connected to the sandbox environment of MCAS. The policies configured in this environment are similar as described in the **Policy Configuration** section of the report. The sandbox environment was monitored for one month to verify the alerts generated by the system. During the experiment, the list of corporate IP addresses, internal and external users, location of admin users was configured to avoid false alerts. During this experiment, the policy threshold for Mass download files were modified based on user behavior. Initially, the policy was designed to download 5 files in one minute, however, after testing and observing user activity, this threshold was increased to 20 file downloads in one minute. Similarly, the threshold for other policies was verified and tested.

The alerts generated were investigated based upon the severity and category of the alert. The alerts generated are in three different categories Threat detection, Sharing controls, and DLP. These alerts were filtered and investigated by considering these categories. The alerts were analyzed and closed by classifying them as True Positive (TP) Bening True Positive (B-TP) or False Positive (FP).[7]

- **True Positive:** If an alert has been issued for a verified malicious activity.
- **Bening:** If an alert is issued for a non malicious activity like pentest or other authorized suspicious actions.
- **False Positive:** If the alert is issued for a non malicious activity.

The image below provides highlights for the alerts generated in this sandbox environment, as well as the geographical location of the users where the activities are performed. The dashboard also displays the number of DLP alerts generated throughout the experiment.

[7] https://docs.microsoft.com/en-us/cloud-app-security/investigate-anomaly-alerts.

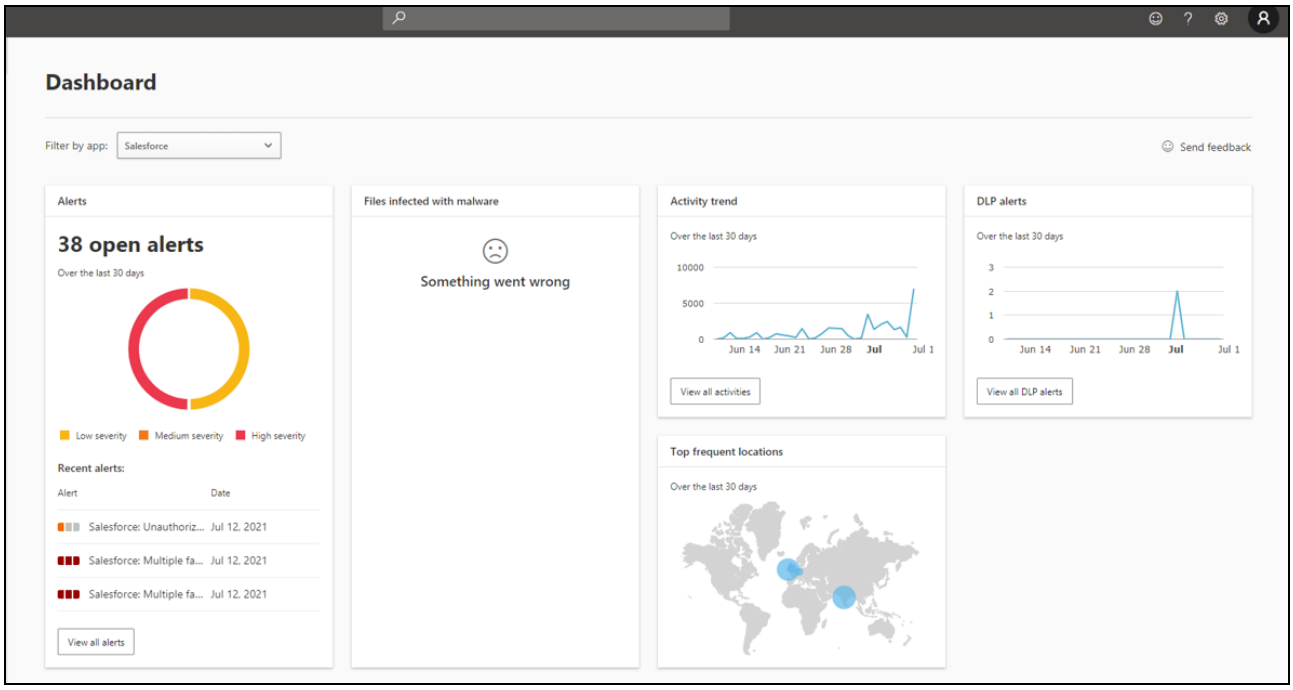

Figure 7: MCAS dashboard on a Sandbox environment

Furthermore, the study conducted in this Sandbox environment highlighted the user's activities, file types utilized in the recruiting environment, and benefited in setting groups and corporate IP addresses to enhance the system's accuracy. This experiment demonstrated how to establish rules with appropriate thresholds. It also provided additional features of DLP, such as configuring policy to find PPSN numbers in a file and detect if the file is exchanged with unauthorized domains. This experiment provided a quantity of information about the activities and events that occurred on the Salesforce platform, which aided in the implementation of the product used in a live environment.

6.2 Testing of the system in Operational Environment

The second phase of testing is performed in the live environment. The Salesforce application is connected to the MCAS. This Salesforce environment is used by the recruitment company to store all user and client data. During this testing phase, there had been a lot of activity in the MCAS environment. These activities include user file uploading, user information updating, file sharing with external users, maintaining user credentials and personal data, etc. All information from these events is collected and analyzed on MCAS for malicious or suspicious actions. The research in this phase followed the same procedure to analyse alerts as in the previous experiment.

Moreover, each alert was analyzed depending on the information revealed by the alerts. These alerts highlighted suspicious behavior with information such as user activity, IP address, device data, application, Geo Location, and even the presence of any critical DLP policy inside the document. Several additional policies were implemented during this phase, such as Files shared with unauthorized domains contains PPSN numbers or IP addresses. The below image highlights the number of files stored on the Slaesforce application. It presents the list of external users with whom the files are shared.

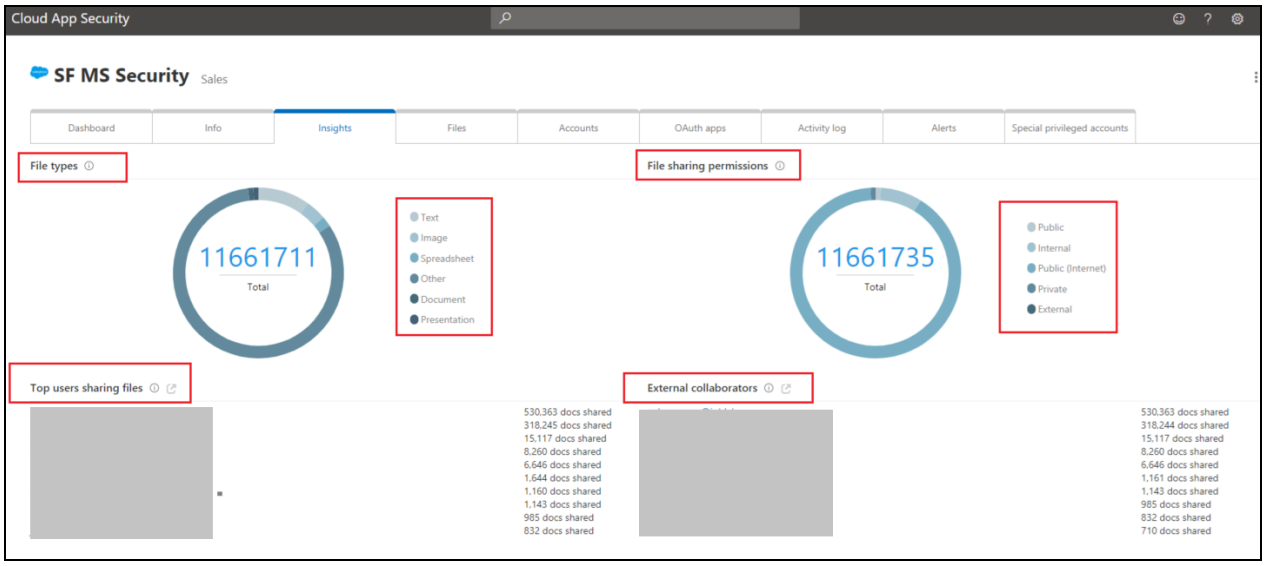

Figure 8: Overview of the Files stored on Salesforce.

The overview of the alerts generated during this experiment is displayed on the Dashboard of the MCAS. This dashboard also presents the activity logs on Salesforce, DLP alerts, and geographical locations from where the activities are performed. The alerts here are displayed based on the severity of the alert.

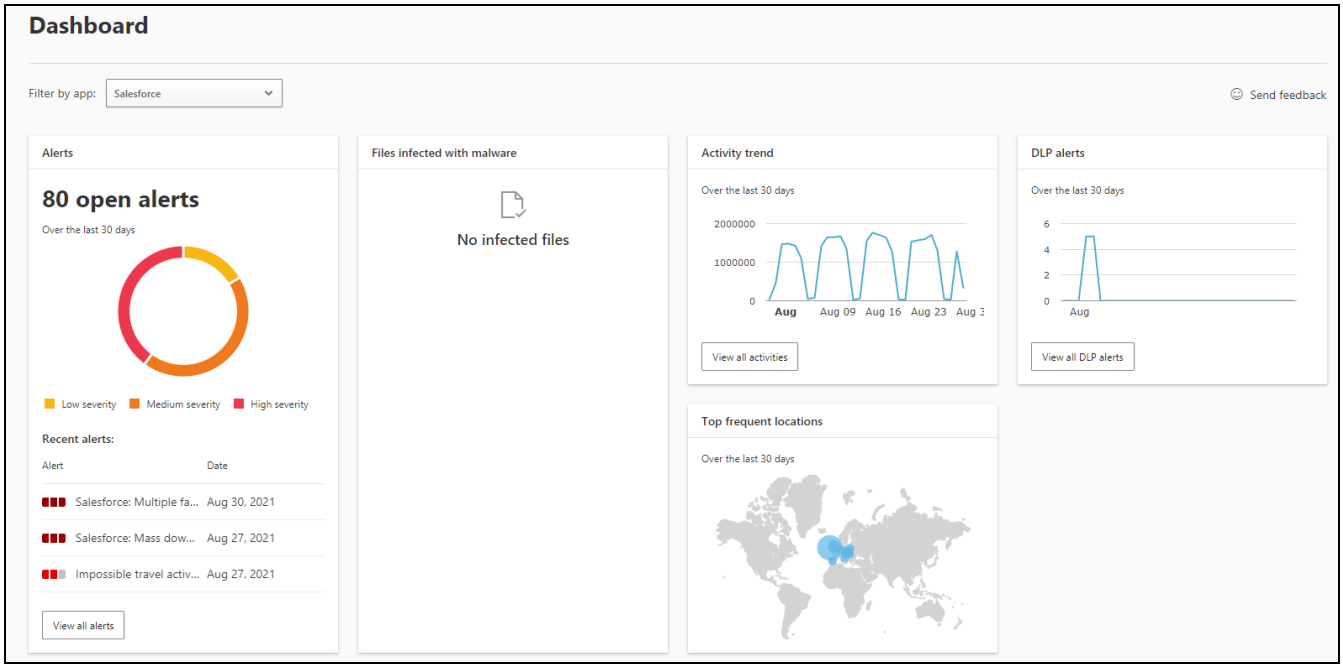

Figure 9: MCAS dashboard on Live environment

6.3 Discussion

On analysing the results obtained from the experiments the developed integrated system can be interpreted as an efficient system in detecting malicious and suspicious activities performed on the data management platform of the recruitment environment. The results obtained from the experiment performed on the Sandbox environment helped in identifying the user groups, the corporate IP address from where the activities are performed and verifying the thresholds for each policy. The second experiment aided in identifying the top

user's IDs who exchange files with external domains as well as detecting malware-infected files obtained by users via spam emails.

Previously established approaches focused solely on the security of IoT devices while ignoring monitoring application-level security and security events on database management systems. This system provides a more efficient way to monitor activities on the database management system of a recruitment company and generating alerts when threats are detected. The designed system can even generate reports of policies that are configured and present statistical data of files that are being exchanged in the recruitment environment.

7 Conclusion and Future Work

The primary objective of this research was to develop an integrated system that can monitor the IT environment in the recruitment company, detect malicious activities, and provide a report of the events detected. The NIST standards helped in the identifying and deployment of the Microsoft Cloud App Security environment for detecting malicious and suspicious activity on the Salesforce platform. The experiments conducted throughout this research not only provided a brief understanding of the data processed in the recruitment environment but also aided in defining the instances where the security must be implemented. This system can be integrated with various Microsoft-supported applications and can be deployed as an in-house SOC system for investigation.

As this system supports multiple applications it can be integrated with O365 apps, multiple network devices to analyze traffic and investigate sensitive information from the files. The system's future work can enable a hybrid method to monitor network and application events in a SOC environment.

References

Schilling, A. and Werners, B. (2016) 'Optimal selection of IT security safeguards from an existing knowledge base', *European Journal of Operational Research*, 248(1), pp. 318–327. doi: 10.1016/j.ejor.2015.06.048.

Weissman, D. and Jayasumana, A. (2020) 'Integrating IoT Monitoring for Security Operation Center', *2020 Global Internet of Things Summit (GIoTS), Global Internet of Things Summit (GIoTS), 2020*, pp. 1–6. doi: 10.1109/GIOTS49054.2020.9119680.

Xu Li and Liu Hongyan (2010) 'Proposal for information security architecture based on a company', *2010 Second International Conference on Communication Systems, Networks and Applications, Communication Systems, Networks and Applications (ICCSNA), 2010 Second International Conference on*, 1, pp. 17–20. doi: 10.1109/ICCSNA.2010.5588795.

Huang, Y. et al. (2019) 'CSAT: A User-interactive Cyber Security Architecture Tool based on NIST-compliance Security Controls for Risk Management', 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), 2019 IEEE 10th Annual, pp. 0697–0707. doi: 10.1109/UEMCON47517.2019.8993090.

Akinrolabu, O., Agrafiotis, I. and Erola, A. (2018) 'The challenge of detecting sophisticated attacks : Insights from SOC Analysts', *Proceedings of the 13th International Conference on Availability, Reliability and Security*. (ACM Other Conferences), pp. 1–9. doi: 10.1145/3230833.3233280.

Bin Hamid Ali, F. A., Jali, M. Z. and bin Nordin, M. N. (2021) 'Preliminary Study on It Security Maintenance Management in Malaysia Organizations', *PalArch's Journal of Archaeology of Egypt/Egyptology*, 18(1), pp. 4061–4073. Available at: https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,cookie,shib&db=edo&AN=149976033&site=eds-live&scope=site (Accessed: 2 September 2021).

Wenjun Cheng, Xiaosu Zhan and Shaohua Zhang (2011) 'Study on service-oriented security architecture', *2011 6th IEEE Joint International Information Technology and Artificial Intelligence Conference, Information Technology and Artificial Intelligence Conference (ITAIC), 2011 6th IEEE Joint International*, 2, pp. 476–479. doi: 10.1109/ITAIC.2011.6030377.

Tafazzoli, T. and Gharaee Garakani, H. (2016) 'Security operation center implementation on OpenStack', 2016 8th International Symposium on Telecommunications (IST), Telecommunications (IST), 2016 8th International Symposium on, pp. 766–770. doi: 10.1109/ISTEL.2016.7881927.

Gupta, N., Traore, I. and de Quinan, P. M. F. (2019) 'Automated Event Prioritization for Security Operation Center using Deep Learning', 2019 IEEE International Conference on Big Data (Big Data), Big Data (Big Data), 2019 IEEE International Conference on, pp. 5864–5872. doi: 10.1109/BigData47090.2019.9006073.

Duan, J., Zhao, B. and Guo, S. (2020) 'The Design and Implementation of Smart Grid SOC Platform', *2020 IEEE International Conference on Information Technology,Big Data and Artificial Intelligence (ICIBA), Information Technology,Big Data and Artificial Intelligence*

(ICIBA), 2020 IEEE International Conference on, 1, pp. 264–268. doi: 10.1109/ICIBA50161.2020.9277373.

Ilya Livshitz, Pavel Lontsikh and Sergey Eliseev (2017) 'The method of implementation of the numerical IT-Security metrics in management systems', *Proceedings of the XXth Conference of Open Innovations Association FRUCT*, 776(20), pp. 242–247. doi: 10.23919/FRUCT.2017.8071318.

Minkevics, V. and Slihte, J. (no date) 'Modelling IT security risk management in academic environment', *Proceedings of the 5th IEEE Workshop on Advances in Information, Electronic and Electrical Engineering, AIEEE 2017*, 2018–January, pp. 1–4. doi: 10.1109/AIEEE.2017.8270562.

Heidenreich, M. (2020) 'Implementation of an IT security measurement method for the evaluation of IT security in micro-enterprises', *2020 International Conference on Computing, Electronics & Communications Engineering (iCCECE), Computing, Electronics & Communications Engineering (iCCECE), 2020 International Conference on*, pp. 92–97. doi: 10.1109/iCCECE49321.2020.9231113.

Soni, K. (1) and Vala, B. (2) (no date) 'Roadmap to salesforce security governance & salesforce access management', *Proceedings of the 2017 2nd IEEE International Conference on Electrical, Computer and Communication Technologies, ICECCT 2017*. doi: 10.1109/ICECCT.2017.8117831.